REMARKS

The Examiner is thanked for the performance of a thorough search. By this amendment, Claims 1, 13, and 15 are amended and Claims 37-42 are added. No claims are canceled or withdrawn. Each issue raised in the Office Action mailed June 18, 2008 is addressed hereinafter.

NEW CLAIMS 37-42

New method claim 37 depends from Claim 1 and features, in part, "wherein said first server and said second server are the same authentication, authorization, and accounting server" and new method claim 38 also depends from Claim 1 and features, in part, "wherein said first server and said second server are different load balanced servers." Thus, Claim 37 covers an embodiment of Claim 1 where the AAA server that sends the claimed "authorization accept message that includes the accounting record" and the AAA server that receives the claimed "start session message that includes the accounting record" are the **same** AAA server. Claim 38, on the other hand, covers an embodiment of Claim 1 where the first AAA server and the second AAA server are **two different load balanced** AAA servers. Adequate support for Claims 37 and 38 can be found throughout the specification including at least in paragraph 54.

New Claims 39-42 are computer-readable storage medium counterpart claims to Claims 35-38 respectively. New Claims 37-42 are allowable over the prior art for at least the reasons provided below.

SUMMARY OF THE REJECTIONS

In the Office Action, Claims 1-2, 4, 6-7, 10-12, 14-15, 17-18, 19, 21, 23-24, 27-29, 31, 32 and 34 were rejected under 35 U.S.C. § 102(e) as allegedly anticipated by U.S. 6,947,725 ("*Aura*").

Claims 3 and 20 were rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over

Aura in view of U.S. Publication 2003/0035409 ("*Wang*").

Claims 5, 8-9, 13, 16, 22, 25, 26, 30, 33, and 35-36 were rejected under 35 U.S.C. §

103(a) as allegedly unpatentable over Aura and U.S. Publication 2002/0046277 ("*Barna*").

These rejections are respectfully traversed.

THE § 102 REJECTIONS OF CLAIMS 1, 2, AND 15

Present Claim 1 features:

A method for improving service accounting in a network, the method comprising the
steps of:
in response to a first authentication, authorization, and accounting server receiving a
    request to authenticate and authorize a client, said first server obtaining **an
    accounting record** for the client and said first server sending an authorization
    accept message that includes the accounting record within the message;
causing the accounting record to be logged; and
a second authentication, authorization, and accounting server receiving, subsequent to the
    sending, a start session message that includes the accounting record.

The Office Action contends that *Aura* anticipates Claim 1. To anticipate Claim 1 *Aura*

must teach each and every of its features. (MPEP § 2131). Since there are several features

recited in Claim 1 that are not taught or suggested by *Aura*, Applicants respectfully submit that

Claim 1 is condition for allowance.

For example, *Aura* does not teach or suggest "in response to a first authentication,

authorization, and accounting server receiving a request to authenticate and authorize a client,

said first server obtaining **an accounting record** for the client and said first server sending an

authorization accept message that includes the accounting record within the message." The

Office Action appears to equate the credential of *Aura* with the accounting record of Claim 1.

However, there are substantial differences between *Aura*'s credential and the claimed accounting record.

For example, in Claim 1, the accounting record is obtained by an authentication, authorization and accounting (AAA) server and sent by the AAA server in an authorization accept message. In contrast, in *Aura*, a mobile node **base station** establishes a credential with a mobile node and the **base station** sends the credential in a secure communication to the mobile node. (*Aura*, col. 5, lines 14-30; fig. 2, item 214 and fig. 3, item 316). Thus, in *Aura*, an AAA server **does not** establish a credential with a mobile node or send a credential to a mobile node, or for that matter, obtain an accounting record and send the accounting record in an authorization accept message.

Aura clearly distinguishes between a base station and an AAA server in its description of a wireless access network. *Aura* states that "the base station 102 or some other communicatively coupled system may access an authentication, authorization, and accounting foreign (AAAF) server to fully authenticate the user." (*Aura*, col. 5, lines 9-12). Further, Fig. 3 of *Aura* shows "Base Station 1" sending communication 312 which represents "an authentication request between the base station 1 and the AAA architecture." (*Aura*, col. 8, lines 61-62). Fig. 3 of *Aura* also shows communication 314 which represents "a grant of access indicated by the AAA architecture to the base station 1." However, as communication 316 of Fig. 3 depicts, it is the base station, <u>and not the AAA architecture</u>, that establishes and sends the credential. Moreover, the "grant of access" communication 314 from the AAA architecture of *Aura* does not include a credential. Thus, the credential of *Aura* does not teach or suggest the accounting record of Claim 1 because the AAA architecture of *Aura* does not obtain the credential and does not send the credential in a communication.

Further, one skilled in the art would not reasonably equate the credential of *Aura* with the accounting record of Claim 1. As described in *Aura*, the credential "informs other entities within the mobile access network 101 (particularly other base stations) that any mobile node that knows the **secret** credential key Kcred (or the **secret part** of the public key P.sub.Kcred) should be trusted for credential authenticated access." (Emphasis added). (*Aura*, col. 5, lines 58-62). Thus, the credential of *Aura* contains **secret** information that should be known only to mobile nodes that are trusted for credential authenticated access. In contrast, the accounting record of Claim 1 contains accounting information that is logged. One skilled in the art would not equate the credential of *Aura* with the accounting record of Claim 1 because to log the credential of *Aura* would potentially expose the secret credential key to elements in the mobile access network that are not trusted for credential authenticated access. Indeed, to log the credential of *Aura* would **destroy one of *Aura's* principles of operation** which is to provide a credential to a mobile node that may be used by other base stations to establish trust with the mobile node. (*Aura*, Abstract). If the secret credential key was exposed in a log, an untrusted network element that has access to the log could read the secret key from the log and use it to acquire unauthorized access to a base station. Consequently, *Aura's* credential does not teach or suggest the claimed accounting record and, in fact, **teaches away** from the claimed accounting record.

The Office Action contends that the feature of Claim 1 reciting "causing the accounting record to be logged" is shown in *Aura* at col. 5, lines 1-30. The entirety of the cited portion of *Aura* is reproduced below for the sake of completeness. From the discussion above, a skilled artisan would not understand *Aura* to provide for logging the credential, because the credential contains secret key information that is used to establish trust between a mobile node and base stations, and exposing such secret information in a log would hinder the ability to establish trust between mobile nodes and base stations. In any event, nowhere in the cited portion of *Aura* or

elsewhere is "logging" the credential described, let alone logging anything equivalent to the

claimed "accounting record."

> At event 110, the mobile node 108 is within the operational zone of the base station 102 and has not previously been authenticated for access to the network 100. Therefore, to access the network, the mobile node 108 attempts a full authentication dialog 122 with the base station 102. If the full authentication operation completes successfully, the mobile node 108 is granted fully authenticated access to the communications network 100 via the base station 102, subject to whatever security policy applies to the authenticated user. This full authentication operation incurs the delay previously discussed. For example, the base station 102 or some other communicatively coupled system may access an authentication, authorization, and accounting foreign (AAAF) server to fully authenticate the user (e.g., through a login validation or an electronic or credit card payment).

> At event 112, the base station 102 establishes a credential key, such as secret credential key Kcred, with the mobile node 108 by sending a credential key to the mobile node 108. (Alternatively, by receiving the credential key from the base station, the mobile node 108 can be said to establish the credential key with the base station). Exemplary methods of establishing the secret credential key with the mobile node 108 include without limitation establishing the secret credential key as part of the authentication process, by using a secure communications link 124 created during the authentication, or by executing a secret key-establishment protocol.

> The base station 102 also sends a credential to the mobile node 108, but this communication need not be over a secure link. The credential may be used by the mobile node 108 to establish credential authenticated access to the network through the base station 104.

(*Aura*, col. 4, line 66 – col. 5, 30). Thus, *Aura* fails to disclose two features of Claim 1: first, "in

response to a first authentication, authorization, and accounting server receiving a request to

authenticate and authorize a client, said first server obtaining **an accounting record** for the

client and said first server sending an authorization accept message that includes the accounting

record within the message," and second, "causing the **accounting record** to be logged."

(Emphases added).

The Office Action equates response 320 of Figure 3 in *Aura* with the "start session

message" of Claim 1. However, as can be seen clearly with reference to Figure 3 of *Aura*, the

response 320 is sent from a mobile node **to a base station** ("Base Station 2"). In contrast, the

"start session message" of Claim 1 is received by an **authentication, authorization, and**

accounting server. The AAA Architecture depicted in Figure 3 of *Aura* does not receive

response 320 sent from the mobile node or anything akin to the claimed "start session message

that includes the accounting record." Thus, *Aura* also does not teach or suggest "a second

authentication, authorization, and accounting server receiving, subsequent to the sending, a start session message that includes the accounting record."

Based on the foregoing, Claim 1 is allowable over *Aura* and removal of the rejection of Claim 1 is respectfully requested. Claim 15 recites features similar to Claim 1 is allowable for the same reasons.

Claim 2 depends from independent claim 1 discussed above. Therefore, Claim 2 is allowable over *Aura* for at least those reasons give above with respect to Claim 1. In addition, Claim 2 introduces additional features that independently render it patentable over *Aura*. For example, Claim 2 features, *inter alia*, "obtaining the accounting record for the client from an external resource."

The Office Action contends that these additional features of Claim 2 are satisfied by *Aura* at fig. 3 steps 312 and 314 and at col. 8, lines 45-68. The cited portion of *Aura* illustrates and describes a base station communicating with one or more servers of an AAA architecture. The cited portion of *Aura* mentions a base station communicating with an AAA server to authenticate a user of a mobile device, but nothing in this portion or elsewhere in *Aura* describes the base station obtaining an accounting record from an AAA server. In communication 312 of Figure 3 of *Aura*, an authentication request is made from the base station to the AAA architecture and a grant of access is indicated in communication 314. One skilled in the art would not reasonably understand an indication of a grant of access as described in *Aura* to be the "accounting record" as claimed.

Moreover, in rejecting Claim 1, the Office Action equates the credential of *Aura* with the claimed "accounting record." Yet, as clearly indicated by Figure 3 of *Aura*, the base station does not obtain the credential from the AAA Architecture. Consequently, Claim 2 recites additional features that independently render it patentable over *Aura*.

THE § 103 REJECTION OF CLAIM 13

In rejecting Claim 13, the Office Action contends that the features of Claim 13 are

satisfied by *Barna* and that the combination of *Aura* and *Barna* satisfy each and every feature of

Claim 13 including the features of Claim 1 from which Claim 13 depends. This is incorrect.

Barna does not overcome the deficiencies of *Aura* identified above. In particular, and as

explained in Applicants' communication filed March 28, 2008, *Barna* does not teach or suggest

"a start session message that includes the accounting record." Specifically, *Barna* says nothing

about receiving a start session message that includes an accounting record that was sent in an

authorization accept message in response to authenticating and authorizing a client. (*See*

Applicants' Reply filed March 28, 2008, pages 12-13). Consequently, the combination of *Aura*

and *Barna* does not teach or suggest the following features of Claim 13:

> wherein the step of said first server sending **an authorization accept message that**
> **includes the accounting record** and the step of said second server receiving **a**
> **start session message that includes the accounting record** are performed in a
> protocol selected from the group consisting of Remote Authentication Dial In
> User Service, Terminal Access Controller Access Control System, Diameter, and
> Security Assertion Markup Language.

(Emphases added). Removal of the rejection of Claim 13 is respectfully requested.

REMAINING CLAIMS

The pending claims not discussed so far are dependant claims that depend on an

independent claim that is discussed above. Because each dependant claim includes the features

of claims upon which they depend, the dependant claims are patentable for at least those reasons

the claims upon which the dependant claims depend are patentable. Removal of the rejections

with respect to the dependant claims and allowance of the dependant claims is respectfully

requested. In addition, the dependent claims introduce additional features that independently

render them patentable. Due to the fundamental differences already identified, a separate

discussion of those features is not included at this time.

CONCLUSION

For the reasons set forth above, it is respectfully submitted that all of the pending claims

are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is

believed next in order, and that action is most earnestly solicited.

The Examiner is respectfully requested to contact the undersigned by telephone if it is

believed that such contact would further the examination of the present application.

Please charge any shortages or credit any overages to Deposit Account No. 50-1302.

Respectfully submitted,

Hickman Palermo Truong & Becker LLP

Date: September 18, 2008   /AdamCStone#60531/
                                                            Adam Christopher Stone
                                                            Reg. No. 60,531

2055 Gateway Place, Suite 550
San Jose, California   95110-1083
Telephone No.: (408) 414-1231
Facsimile No.: (408) 414-1076